P⊗RTAL

USPTO

Search: ⊙ The ACM Digital Library   ○ The Guide

pre boot$4 and post boot$4 security ((operating system) or OS   **SEARCH**

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **pre boot$4** and **post boot$4** **security operating system** or **OS**   Found **80,196** of **204,472**

Sort results by   relevance ▼

Display results   expanded form ▼

🔖 Save results to a Binder

❓ Search Tips

☐ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next
Best 200 shown   Relevance scale ☐▭▬■■

1 IS '97: model curriculum and guidelines for undergraduate degree programs in information systems
Gordon B. Davis, John T. Gorgone, J. Daniel Couger, David L. Feinstein, Herbert E. Longenecker
December 1996 **ACM SIGMIS Database , Guidelines for undergraduate degree programs on Model curriculum and guidelines for undergraduate degree programs in information systems IS '97,** Volume 28 Issue 1
Publisher: ACM Press
Full text available: 📄 pdf(7.24 MB)   Additional Information: full citation, citings

2 Software security: Application security support in the operating system kernel
Manigandan Radhakrishnan, Jon A. Solworth
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: 📄 pdf(335.52 KB)   Additional Information: full citation, abstract, references, cited by, index terms

Application security is typically coded in the application. In *kernelSec,* we are investigating mechanisms to implement application security in an operating system kernel. The mechanisms are oriented towards providing authorization properties, and this goal drives the design of permissions and protection mechanisms.The resulting system is dynamic, allowing the set of permissions for a program to evolve during program execution. This reduces the need for users and applications to be aware o ...

Keywords: access controls, authorization, authorization properties, information flow, operating systems, separation of duty

3 Analysis and verification: MECA: an extensible, expressive system and language for statically checking security properties
Junfeng Yang, Ted Kremenek, Yichen Xie, Dawson Engler
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**
Publisher: ACM Press
Full text available: 📄 pdf(343.82 KB)   Additional Information: full citation, abstract, references, citings, index terms

This paper describes a system and annotation language, MECA, for checking security rules. MECA is expressive and designed for checking real systems. It provides a variety of practical constructs to effectively annotate large bodies of code. For example, it allows programmers to write programmatic annotators that automatically annotate large bodies of source code. As another example, it lets programmers use general predicates to determine if an annotation is applied; we have used this ability to ...

Keywords: annotation language, static analysis

4 MANTIS OS: an embedded multithreaded operating system for wireless micro sensor platforms

Shah Bhatti, James Carlson, Hui Dai, Jing Deng, Jeff Rose, Anmol Sheth, Brian Shucker, Charles Gruenwald, Adam Torgerson, Richard Han

August 2005 **Mobile Networks and Applications,** Volume 10 Issue 4

Publisher: Kluwer Academic Publishers

Full text available: pdf(1.27 MB)   Additional Information: full citation, abstract, references, index terms

The MANTIS MultimodAl system for NeTworks of In-situ wireless Sensors provides a new multithreaded cross-platform embedded operating system for wireless sensor networks. As sensor networks accommodate increasingly complex tasks such as compression/aggregation and signal processing, preemptive multithreading in the MANTIS sensor OS (MOS) enables micro sensor nodes to natively interleave complex tasks with time-sensitive tasks, thereby mitigating the bounded buffer producer-consumer problem. To ac ...

Keywords: cross-platform, dynamic reprogramming, embedded operating system, lightweight, low power, multithreaded, sensor networks

5 Session 31: secure systems: VIRTUS: a new processor virtualization architecture for security-oriented next-generation mobile terminals

Hiroaki Inoue, Akihisa Ikeno, Masaki Kondo, Junji Sakai, Masato Edahiro

July 2006   **Proceedings of the 43rd annual conference on Design automation DAC '06**

Publisher: ACM Press

Full text available: pdf(798.11 KB)   Additional Information: full citation, abstract, references, index terms

We propose a new processor virtualization architecture, VIRTUS, to provide a dedicated domain for pre-installed applications and virtualized domains for downloaded native applications. With it, security-oriented next-generation mobile terminals can provide any number of domains for native applications. VIRTUS features three new technologies: VMM asymmetrization, dynamic inter-domain communication and virtualization-assist logic, and it is first in the world to virtualize an ARM-based multiproces ...

Keywords: multiprocessor, processor virtualization

6 Session 3: Energy-aware OS's: Every joule is precious: the case for revisiting operating system design for energy efficiency

Amin Vahdat, Alvin Lebeck, Carla Schlatter Ellis

September 2000 **Proceedings of the 9th workshop on ACM SIGOPS European workshop: beyond the PC: new challenges for the operating system EW 9**

Publisher: ACM Press

Full text available: pdf(71.97 KB)   Additional Information: full citation, abstract, references, citings

By some estimates, there will be close to one billion wireless devices capable of Internet connectivity within five years, surpassing the installed base of traditional wired compute devices. These devices will take the form of cellular phones, personal digital assistants (PDA's), embedded processors, and "Internet appliances". This proliferation of networked computing devices will enable a number of compelling applications, centering around ubiquitous access to global information serv ...

7 Session summaries from the 17th symposium on operating systems principle (SOSP'99)

Jay Lepreau, Eric Eide

April 2000   **ACM SIGOPS Operating Systems Review,** Volume 34 Issue 2

Publisher: ACM Press

Full text available: pdf(3.15 MB)   Additional Information: full citation, index terms

8 Digest of proceedings seventh IEEE workshop on hot topics in operating systems March 29-30 1999, Rio Rico, AZ

M. Satyanarayanan

October 1999 **ACM SIGOPS Operating Systems Review,** Volume 33 Issue 4

Publisher: ACM Press
Full text available: pdf(1.67 MB)   Additional Information: full citation, abstract, index terms

The Seventh IEEE Workshop on Hot Topics in Operating Systems was held on March 29-30 1999 at the Rio Rico Resort & Country Club, south of Tucson, Arizona. The General Chair, Peter Druschel, and the Local Arrangements Chair, John Hartman, had gone to considerable effort to make the operation of the workshop smooth and pleasant for the participants. The secluded desert locale, the effect of brilliant sunshine and blue skies on winter-jaded northerners, and the enthusiasm and energy of the ...

9   Security and eliability: Live updating operating systems using virtualization
Haibo Chen, Rong Chen, Fengzhe Zhang, Binyu Zang, Pen-Chung Yew
June 2006   **Proceedings of the second international conference on Virtual execution environments VEE '06**
Publisher: ACM Press
Full text available: pdf(136.71 KB)   Additional Information: full citation, abstract, references, index terms

Many critical IT infrastructures require non-disruptive operations. However, the operating systems thereon are far from perfect that patches and upgrades are frequently applied, in order to close vulnerabilities, add new features and enhance performance. To mitigate the loss of availability, such operating systems need to provide features such as live update through which patches and upgrades can be applied without having to stop and reboot the operating system. Unfortunately, most current live ...

Keywords: availability, live update, operating system, virtualization

10   Applications and compliance: Virtual monotonic counters and count-limited objects using a TPM without a trusted OS
Luis F. G. Sarmenta, Marten van Dijk, Charles W. O'Donnell, Jonathan Rhodes, Srinivas Devadas
November 2006 **Proceedings of the first ACM workshop on Scalable trusted computing STC '06**
Publisher: ACM Press
Full text available: pdf(447.59 KB)   Additional Information: full citation, abstract, references, index terms

A trusted monotonic counter is a valuable primitive that enables a wide variety of highly scalable offline and decentralized applications that would otherwise be prone to replay attacks, including offline payment, e-wallets, virtual trusted storage, and digital rights management (DRM). In this paper, we show how one can implement a very large number of *virtual* monotonic counters on an untrusted machine with a Trusted Platform Module (TPM) or similar device, without relying on a trusted OS ...

Keywords: certified execution, e-wallet memory integrity checking, key delegation, stored-value, trusted storage

11   Operating systems: *t-kernel*: providing reliable OS support to wireless sensor networks
Lin Gu, John A. Stankovic
October 2006 **Proceedings of the 4th international conference on Embedded networked sensor systems SenSys '06**
Publisher: ACM Press
Full text available: pdf(524.19 KB)   Additional Information: full citation, abstract, references, index terms

The development of a reliable large-scale wireless sensor network (WSN) is very difficult because of resource constraints, energy budget, and demanding application requirements. Three OS features-OS protection, virtual memory, and preemptive scheduling-can significantly improve the reliability of WSN systems and facilitate developing complex WSN software. However, due to the lack of hardware support for privileged execution and address translation, it is impossible to implement these features wi ...

Keywords: OS protection, binary translation, low-power systems, virtual memory, wireless sensor networks

12   Security: Raksha: a flexible information flow architecture for software security
Michael Dalton, Hari Kannan, Christos Kozyrakis

June 2007   **Proceedings of the 34th annual international conference on Computer architecture ISCA '07**

Publisher: ACM Press

Full text available: pdf(300.74 KB)   Additional Information: full citation, abstract, references, index terms

High-level semantic vulnerabilities such as SQL injection and crosssite scripting have surpassed buffer overflows as the most prevalent security exploits. The breadth and diversity of software vulnerabilities demand new security solutions that combine the speed and practicality of hardware approaches with the flexibility and robustness of software systems.

This paper proposes Raksha, an architecture for software security based on dynamic information flow tracking (DIFT). Raksha provide ...

Keywords: dynamic, semantic vulnerabilities, software security

13   Labels and event processes in the asbestos operating system

Petros Efstathopoulos, Maxwell Krohn, Steve VanDeBogart, Cliff Frey, David Ziegler, Eddie Kohler, David Mazières, Frans Kaashoek, Robert Morris

October 2005   **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5

Publisher: ACM Press

Full text available: pdf(258.58 KB)   Additional Information: full citation, abstract, references, citings, index terms

Asbestos, a new prototype operating system, provides novel labeling and isolation mechanisms that help contain the effects of exploitable software flaws. Applications can express a wide range of policies with Asbestos's kernel-enforced label mechanism, including controls on inter-process communication and system-wide information flow. A new event process abstraction provides lightweight, isolated contexts within a single process, allowing the same process to act on behalf of multiple users while ...

Keywords: event processes, information flow, labels, mandatory access control, secure web servers

14   Security and eliability: A feather-weight virtual machine for windows applications

Yang Yu, Fanglu Guo, Susanta Nanda, Lap-chung Lam, Tzi-cker Chiueh

June 2006   **Proceedings of the second international conference on Virtual execution environments VEE '06**

Publisher: ACM Press

Full text available: pdf(192.18 KB)   Additional Information: full citation, abstract, references, index terms

Many fault-tolerant and intrusion-tolerant systems require the ability to execute unsafe programs in a realistic environment without leaving permanent damages. Virtual machine technology meets this requirement perfectly because it provides an execution environment that is both realistic and isolated. In this paper, we introduce an OS level virtual machine architecture for Windows applications called *Feather-weight Virtual Machine* (FVM), under which virtual machines share as many resources ...

Keywords: copy on write, mobile code security, namespace virtualization, system call interception, virtual machine

15   Operating system enhancements to prevent the misuse of system calls

Massimo Bernaschi, Emanuele Gabrielli, Luigi V. Mancini

November 2000   **Proceedings of the 7th ACM conference on Computer and communications security CCS '00**

Publisher: ACM Press

Full text available: pdf(413.22 KB)   Additional Information: full citation, references, citings, index terms

Keywords: Linux, access control database, buffer overflow based attacks, isolation, system calls interception

16   Selected writings on computing: a personal perspective

Edsger W. Dijkstra
January 1982 Book

Publisher: Springer-Verlag New York, Inc.

Full text available: pdf(60.98 MB)   Additional Information: full citation, abstract, references, cited by, index terms

Since the summer of 1973, when I became a Burroughs Research Fellow, my life has been very different from what it had been before. The daily routine changed: instead of going to the University each day, where I used to spend most of my time in the company of others, I now went there only one day a week and was most of the time that is, when not travelling!-- alone in my study. In my solitude, mail and the written word in general became more and more important. The circumstance that my employe ...

17   Bugs as deviant behavior: a general approach to inferring errors in systems code

Dawson Engler, David Yu Chen, Seth Hallem, Andy Chou, Benjamin Chelf
October 2001 **ACM SIGOPS Operating Systems Review , Proceedings of the eighteenth ACM symposium on Operating systems principles SOSP '01**, Volume 35 Issue 5

Publisher: ACM Press

Full text available: pdf(1.53 MB)   Additional Information: full citation, abstract, references, citings, index terms

A major obstacle to finding program errors in a real system is knowing what correctness rules the system must obey. These rules are often undocumented or specified in an ad hoc manner. This paper demonstrates techniques that automatically extract such checking information from the source code itself, rather than the programmer, thereby avoiding the need for a priori knowledge of system rules.The cornerstone of our approach is inferring programmer "beliefs" that we then cross-check for contradict ...

18   Operating systems security: Gray-box extraction of execution graphs for anomaly detection

Debin Gao, Michael K. Reiter, Dawn Song
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**

Publisher: ACM Press

Full text available: pdf(254.75 KB)   Additional Information: full citation, abstract, references, citings, index terms

Many host-based anomaly detection systems monitor a process by observing the system calls it makes, and comparing these calls to a model of behavior for the program that the process should be executing. In this paper we introduce a new model of system call behavior, called an <i>execution graph</i>. The execution graph is the first such model that both requires no static analysis of the program source or binary, and conforms to the control flow graph of the program. When used as the m ...

Keywords: anomaly detection, control flow graph, intrusion detection, system call monitor

19   Security: New cache designs for thwarting software cache-based side channel attacks

Zhenghong Wang, Ruby B. Lee
June 2007 **Proceedings of the 34th annual international conference on Computer architecture ISCA '07**

Publisher: ACM Press

Full text available: pdf(511.90 KB)   Additional Information: full citation, abstract, references, index terms

Software cache-based side channel attacks are a serious new class of threats for computers. Unlike physical side channel attacks that mostly target embedded cryptographic devices, cache-based side channel attacks can also undermine general purpose systems. The attacks are easy to perform, effective on most platforms, and do not require special instruments or excessive computation power. In recently demonstrated attacks on software implementations of ciphers like AES and RSA, the full key can ...

Keywords: cache, computer architecture, processor, security, side channel, timing attacks

20   Formalizing the safety of Java, the Java virtual machine, and Java card

Pieter H. Hartel, Luc Moreau
December 2001

ACM Computing Surveys (CSUR), Volume 33 Issue 4

Publisher: ACM Press

Full text available: pdf(442.86 KB)   Additional Information: full citation, abstract, references, citings, index terms

We review the existing literature on Java safety, emphasizing formal approaches, and the impact of Java safety on small footprint devices such as smartcards. The conclusion is that although a lot of good work has been done, a more concerted effort is needed to build a coherent set of machine-readable formal models of the whole of Java and its implementation. This is a formidable task but we believe it is essential to build trust in Java safety, and thence to achieve ITSEC level 6 or Common Crite ...

Keywords: Common criteria, programming

Results 1 - 20 of 200   Result page: **1**   2   3   4   5   6   7   8   9   10   next

IEEE Xplore®
RELEASE 2.3

Search Result - Print Format

Key: IEEE JNL = IEEE Journal or Magazine, IEE JNL = IEE Journal or Magazine, IEEE CNF = IEEE Conference, II
CNF = IEE Conference, IEEE STD = IEEE Standard

1. **Malicious code detection for open firmware**
   Adelstein, F.; Stillerman, M.; Kozen, D.;
   Computer Security Applications Conference, 2002. Proceedings. 18th Annual
   9-13 Dec. 2002 Page(s):403 - 412
   IEEE CNF

2. **Enhancing PC Security with a U-Key**
   Peng Shaunghe; Han Zhen;
   Security & Privacy Magazine, IEEE
   Volume 4, Issue 5, Sept.-Oct. 2006 Page(s):34 - 39
   IEEE JNL

3. **A case study of secure ATM switch booting**
   Chuang, S.-C.; Roe, M.;
   Network and Distributed System Security, 1996., Proceedings of the Symposium on
   22-23 Feb. 1996 Page(s):103 - 112
   IEEE CNF

4. **Alien vs. Quine**
   Gratzer, Vanessa; Naccache, David;
   Security & Privacy Magazine, IEEE
   Volume 5, Issue 2, March-April 2007 Page(s):26 - 31
   IEEE JNL

5. **Building the IBM 4758 secure coprocessor**
   Dyer, J.G.; Lindemann, M.; Perez, R.; Sailer, R.; van Doorn, L.; Smith, S.W.;
   Computer
   Volume 34, Issue 10, Oct. 2001 Page(s):57 - 66
   IEEE JNL

6. **Software boot camps are in, and focused on security**
   Cole, B.;
   Software, IEEE
   Volume 22, Issue 3, May-June 2005 Page(s):112
   IEEE JNL

7. **JTRS applications to DoD programs: technology and implementation**
   Cooper, D.M.; Prill, R.; Horihan, G.;
   MILCOM 2002. Proceedings
   Volume 2, 7-10 Oct. 2002 Page(s):1427 - 1432 vol.2
   IEEE CNF

8. **Secure Bit: Transparent, Hardware Buffer-Overflow Protection**
   Enbody, R.J.; Piromsopa, K.;
   Dependable and Secure Computing, IEEE Transactions on
   Volume 3, Issue 4, Oct.-Dec. 2006 Page(s):365 - 376
   IEEE JNL

9. **Applying protocol analysis to security device interfaces**
Herzog, J.;
Security & Privacy Magazine, IEEE
Volume 4, Issue 4, July-Aug. 2006 Page(s):84 - 87
IEEE JNL

10. **Energy and Execution Time Analysis of a Software-based Trusted Platform Module**
Aaraj, Najwa; Raghunathan, Anand; Ravi, Srivaths; Jha, Niraj K.;
Design, Automation & Test in Europe Conference & Exhibition, 2007. DATE '07
April 2007 Page(s):1 - 6
IEEE CNF

11. **Implementation of 10Gb Ethernet Switch Hardware Platform with a Network Processor and a 10Gb EMAC**
Lee, Sang-Woo; Jeon, Yong-Sung; Kim, Ki-Young; Jang, Jong-Soo;
Advanced Communication Technology, The 9th International Conference on
Volume 1, Feb. 2007 Page(s):563 - 566
IEEE CNF

12. **FIDES: an advanced chip multiprocessor platform for secure next generation mobile terminals**
Kondo, M.; Edahiro, M.; Ikeno, A.; Sakai, J.; Inoue, H.;
Hardware/Software Codesign and System Synthesis, 2005. CODES+ISSS '05. Third IEEE/ACM/IFIP International
Conference on
Sept. 2005 Page(s):178 - 183
IEEE CNF

13. **Implementation of VPN Router Hardware Platform using Network Processor**
Sang-Woo Lee; Yong-Sung Jeon; Ki-Young Kim; Jong-Soo Jang;
Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference
Volume 1, 20-22 Feb. 2006 Page(s):671 - 674
IEEE CNF

14. **The Laundromat Model for Autonomic Cluster Computing**
Hansen, J.G.; Christiansen, E.; Jul, E.;
Autonomic Computing, 2006. ICAC '06. IEEE International Conference on
13-16 June 2006 Page(s):114 - 123
IEEE CNF

15. **High performance computing environments without the fuss: the Bootable Cluster CD**
Diesburg, S.M.; Gray, P.A.; Joiner, D.;
Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International
4-8 April 2005 Page(s):8 pp.
IEEE CNF

16. **Integrating Linux into a Windows-based campus network: modifying open source/free software in support ᴏ
the computer science curriculum**
Blankenheim, K.R.; Tate, R.;
Frontiers in Education, 2003. FIE 2003. 33rd Annual
Volume 2, 5-8 Nov. 2003 Page(s):F3C - 9-11 Vol.2
IEEE CNF

17. **Design and implementation of the Trusted BSD MAC framework**
Watson, R.; Feldman, B.; Migus, A.; Vance, C.;
DARPA Information Survivability Conference and Exposition, 2003. Proceedings
Volume 1, 22-24 April 2003 Page(s):38 - 49 vol.1
IEEE CNF

18. **The virtual cluster: a dynamic network environment for exploitation of idle resources**

De Rose, C.; Blanco, F.; Maillard, N.; Saikoski, K.; Novaes, R.; Richard, O.; Richard, B.;
Computer Architecture and High Performance Computing, 2002. Proceedings. 14th Symposium on
28-30 Oct. 2002 Page(s):141 - 148
IEEE CNF

19. **Spy: a method to secure clients for network services**
Lipton, R.J.; Rajagopalan, S.; Serpanos, D.N.;
Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on
2-5 July 2002 Page(s):23 - 28
IEEE CNF

20. **The use of automatic number plate recognition reading in managing access to the boots company headquarter site**
Davidson, S.;
Security Technology, 2001 IEEE 35th International Carnahan Conference on
16-19 Oct. 2001 Page(s):52 - 53
IEEE CNF

21. **Krypton-Crypto-based access control system**
Spesivtsev, A.V.; Krutjakov, A.J.; Seregin, V.V.; Sidorov, V.A.; Wegner, V.A.;
Security Technology, 1992. Crime Countermeasures, Proceedings. Institute of Electrical and Electronics Engineers 1992 International Carnahan Conference on
14-16 Oct. 1992 Page(s):169 - 171
IEEE CNF

22. **Remote booting in a hostile world: to whom am I speaking? [Computer security]**
Lomas, M.; Christianson, B.;
Computer
Volume 28, Issue 1, Jan. 1995 Page(s):50 - 54
IEEE JNL

23. **Understanding trusted computing: will its benefits outweigh its drawbacks?**
Felten, E.W.;
Security & Privacy Magazine, IEEE
Volume 1, Issue 3, May-June 2003 Page(s):60 - 62
IEEE JNL

24. **Khnum - a scalable rapid application deployment system for dynamic hosting infrastructures**
Azagury, A.; Goldszmidt, G.; Koren, Y.; Rochwerger, B.; Tal, A.;
Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium on ·
24-28 March 2003 Page(s):307 - 320
IEEE CNF

Google

securing preboot during post boot | Search | Advanced Search
Preferences

Web   Results **1 - 10** of about **67,500** for **securing preboot during post boot**. (0.10 seconds)

Method for securing communications in a pre-boot environment ...
securing the communication link, **during a pre-boot** operational state prior to ..... system
negotiating a **security** association **during** a **post-boot** operational ...
www.freepatentsonline.com/6327660.html - 54k - Cached - Similar pages

Method and apparatus for execution of an application during ...
Method and apparatus for execution of an application **during** computer **pre-boot** operation
and **post-boot** under normal OS control. Document Type and Number: ...
www.freepatentsonline.com/6564318.html - 57k - Cached - Similar pages
[More results from www.freepatentsonline.com]

[PDF] LNCS 3072 - Biometric User Authentication for Heightened ...
File Format: PDF/Adobe Acrobat
Section 3 compares the **security** threats of **pre-boot**. and **post-boot** authentications ....
protect the data before and **during** transmission through the network. ...
www.springerlink.com/index/9lj6afrwe2rv7cce.pdf - Similar pages

Method and apparatus for execution of an application during ...
... execution of an application **during** computer **pre-boot** operation and **post-boot** under
normal OS ... Method and apparatus for real-time **secure** file deletion ...
www.patentstorm.us/patents/6564318.html - 19k - Cached - Similar pages

SafeNet ProtectDrive
ProtectDrive is hard disk encryption software for **securing** sensitive data. ProtectDrive
provides **pre-boot** authentication and once installed, encrypts and ...
www.safenet-inc.com/products/data_at_rest_protection/Protectdrive_QFacts.asp - 22k -
Cached - Similar pages

General Software's Boot Security -- Chain of Trust between POST ...
In fact, it provides the essential **pre-boot security** checkpoint that ensures that ... **During**
the system's steady state, this application receives periodic ...
www.gensw.com/pages/prod/fwapp/bootsec.htm - 16k - Cached - Similar pages

General Software's Platform Update Facility -- Automatic In-Field ...
It can operate in the **pre-boot** environment **during POST**, or when the OS is ... (as
determined by either Platform Update or the **Boot Security** application) or ...
www.gensw.com/pages/prod/fwapp/puf.htm - 17k - Cached - Similar pages
[More results from www.gensw.com]

[PDF] Embedding browser technology into the Framework
File Format: PDF/Adobe Acrobat - View as HTML
Securing Pre-Boot Applications. **Security** in the Framework ... —is not directly related to
POST/O.S. Load. —otherwise performs a task, e.g.: ...
download.intel.com/technology/efi/docs/pdfs/EFIS004spr05.pdf - Similar pages

[PDF] Slide 1

File Format: PDF/Adobe Acrobat - View as HTML
Executed **during POST**, before OS **boot** ... PXE provides a **pre-boot** means of using the
network ... TPM with **secure** bootstrap prevents this class of attack ...

---

www.ngssoftware.com/research/papers/BH-DC-07-Heasman.pdf - Similar pages

[PDF] ProtectDrive
File Format: PDF/Adobe Acrobat - View as HTML
environment enabling single sign-on to Windows.This means that once the user has been
successfully authenticated **during** the. **pre-boot** authentication process ...
www.safenet - inc.com/Library/3/PDrive_A4.pdf - Similar pages

1 2 3 4 5 6 7 8 9 10   **Next**

Try Google Desktop: search your computer as easily as you search the web.

| securing preboot during post boot | | Search |

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---

©2007 Google - Google Home - Advertising Programs - Business Solutions - About Google

Google

| post boot accessing preboot (descriptor or "res | Search | Advanced Search
                                                                   Preferences

Try uppercase **"OR"** to search for either of two terms. [details]

Web   Results **1** - **1** of **1** for **post** **boot** **accessing** preboot (**descriptor** or "**resource** **protection** **list**"). **(0.29** seconds)

Tip: Try removing quotes from your search to get more results.

Methods and apparatus to provide protection for firmware resources ...
[0025] Protection **descriptors** are communicated to the **post-boot** environment 101
by handing off the **resource protection list** 108 from the **pre-boot** ...
www.freepatentsonline.com/20050114687.html - 74k - Cached - Similar pages

Try Google Desktop: search your computer as easily as you search the web.

_____

| post boot accessing preboot (descri | Search |

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

_____

©2007 Google - Google Home - Advertising Programs - Business Solutions - About Google